HADMÉRNÖK

IV. Évfolyam 4. szám - 2009. december

Varga Péter
varga.peter@kvk.bmf.hu

Illési Zsolt
illesi.zsolt@proteus.hu

KRITIKUS INFRASTRUKTÚRÁK HATÁS ALAPÚ MODELLEZÉSE

Absztrakt

A gazdaság dinamikus fejlődéséhez nagyban hozzájárult az informatika és a telekommunikáció térhódítása. Már nem tudunk elképzelni olyan modern munkaállomást, ahol a dolgozó munkáját valamilyen technikai vívmány ne segítené. Nincs ez máshogyan a kritikus infrastruktúrákban sem. A fenyegetések minimalizálására több módszer alkalmazható. Ezek közé tartozik a kockázatelemzés, mely valószínűségi számításokat, matematikai logikát, kvantitatív, kvalitatív módszerek tartalmazhat. A technika és az általa nyújtott szolgáltatás nem csak az adott infrastruktúrát hálózza be, hanem az infrastruktúra nyújtotta szolgáltatásai révén szoros kapcsolatban (függésben) van más infrastruktúrákkal is. A kritikus infrastruktúrák közötti függéseket, illetve egy kritikus infrastruktúrán belüli függéseket azonban ezek a modellek nem, vagy csak nagyon áttételesen érintik. Ezért cikkünkben egy olyan rendszerszemléletű modellt alkotunk meg, amely alkalmas az inter- és intradependenciák modellezésére, a függőségek tartalmának feltérképezésére.

The penetration of information technology and telecommunication contributed considerably to the dynamic development of the economy. An up to date workstation is unthinkable without technologically advanced tools helping the workers. This is the same in the critical infrastructure domain. There are multiple ways to minimise threats. One of this methods is risk assessment, which utilises probability calculations, mathematical logic, qualitative and quantitative technique. Technology and the provided services not only spreading through a given infrastructure, but via the services provided by the infrastructure it is in close links (dependence) with other infrastructures. The interdependence between critical infrastructures and internal dependencies within a critical infrastructure in these models are not included, or only superficially exposed. Therefore we are suggesting a system approach model which is applicable to prototyping inter- and intradependencies and mapping the background of dependencies.

Kulcsszavak: *kritikus infrastruktúra (KI), hatás alapú modellezés, KI interdependencia, KI intradependencia ~ critical Inftastructure (CI), effect-based modelling, CI interdependence, CI intradependence*

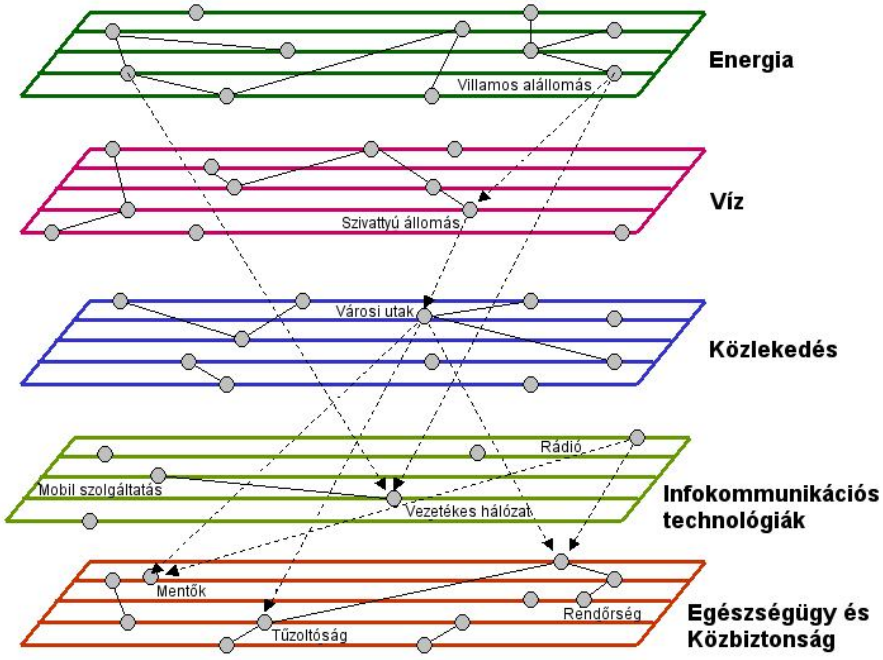
BEVEZETÉS

Az infokommunikáció térnyerése egyre nyilvánvalóbbá tette az infokommunikációs technológiák és ezzel párhuzamosan a természet- és társadalomtudományok fejlődését. A társadalomban és a gazdasági életben is egyre elterjedtebb az informatika, a telekommunikáció. A gyorsabb, intenzívebb változások megnövelték a társadalom technológiai függését, növekedtek a változásokban rejlő lehetőségek és potenciális veszélyek is. [6]

A kritikus infrastruktúrák (KI) és ezen belül a kritikus információs infrastruktúrák (KII) azonosítása, priorizálása, a veszélyeik és sérülékenységeik felmérése, a védelmi terveik meghatározása és kialakítása egyre égetőbb kérdés, és számos országban – így hazánkban is – komoly kihívást jelent.

A KI védelmének kialakításakor a kockázatok felmérésének egyik lényeges pontja a KI-KI interdependenciák (kölcsönös függőség), és az egyes KI-ken belüli intradependenciák (belső rendszerelemtől való függőség) feltárása, valamint a függőség jellegének és tartalmának feltárása, hiszen ezek kezelése csak megfelelő előismeretek birtokában teszi az inter- és intradependenciát csökkentő védelmet teljes körűvé, zárttá és kockázatarányossá.

A kritikus infrastruktúrák védelmi képességeinek beazonosításakor nem minden esetben történik meg az inter- és intradependencia totális feltérképezése. Nem könnyű ezt a feladatot elvégezni, mert a modellezés során figyelembe kell venni a különböző szervezeteket, rendszereket és alrendszereket, illetve ezek kölcsönös kapcsolatrendszerét. A modellezés az az első lépés, amellyel közelebb kerülhetünk a helyes megoldáshoz. Az 1. ábra New Orleans KI ágazatait és az alágazatok közti kapcsolatokat mutatja be:



1. ábra. New Orleans infrastruktúra interdependenciái [4: p 3.]

A Katrina hurrikán megmutatta, hogy az összekapcsolódó infrastruktúrákon keresztül a problémák felhalmozódhatnak, váratlanabb és lényegesen súlyosabb működésbeli zavart

okozhatnak az adott állam létfontosságú szolgáltatásaiban. Az infrastruktúrák összekapcsolódásai, és egymástól való függőségei sérülékenyebbé teszi őket támadások, zavarok, megsemmisítésre irányuló tevékenységekkel szemben. Például az energiatermelés függ a szállítástól. A szállítás függ az energiától. Mindkettő függ az infokommunikációs rendszerektől, míg az infokommunikációs rendszerek energiafüggők. [3]

A kritikus infrastruktúrák védelme elsődleges szempont minden nemzet számára. Ma Magyarországon a Zöld Könyv alapján a nemzeti kritikus infrastruktúra védelem végrehajtásának lépései a következők:

- fogalmak tisztázása, keretrendszer alapjainak meghatározása;
- szektorelemzés, ágazati fogalmak, kritériumok meghatározása;
- kölcsönös függőség (interdependencia elemzés);
- kockázat, veszély, és sebezhetőség elemzés;
- védelmi intézkedések megtétele;
- végrehajtás ellenőrzése és értékelés. [1]

Ebből a felsorolásból is jól látszik, hogy a kölcsönös függőségek elemzése, fontos pillére az infrastruktúrák védelmének. Az inter- és intradependenciák hatékony és eredményes feltárásához, értékeléséhez azonban rendszerszemléletű modell megalkotása szükséges.

Jelen cikkünkben egy ilyen lehetséges modellt szeretnénk felvázolni, azonosítva a KI függőségi rendszer modellezéséhez szükséges főbb paramétereket. A célunk továbbá az, hogy a KI függőségei modell és a kockázatelemzési modell közös illetve eltérő sajátosságaira is rávilágítsunk.

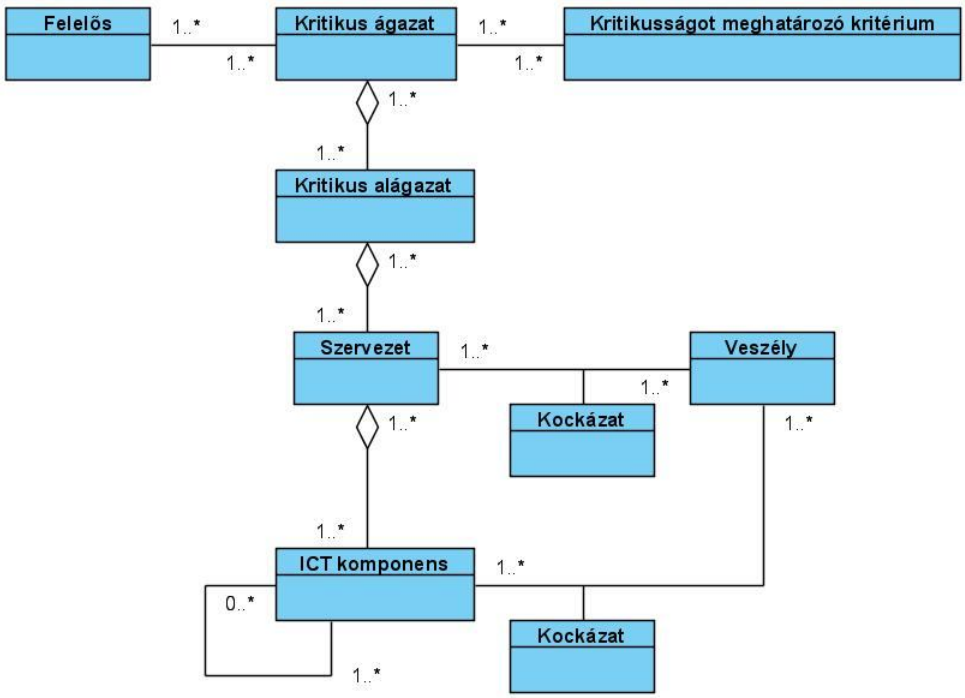
KRITIKUS INFRASTRUKTÚRA FÜGGŐSÉGÉNEK MODELL ELEMEI

A KI-KI függőségi modellben szerepelni kell a KI hierarchiának, vagyis a nemzetközi, nemzeti, EU KI elemeknek, továbbá azonosítania kell az egyedi KI szervezeteket, kapcsolódnia kell a 2080/2008. (VI. 30.) Korm. határozatban felvázolt kritikus ágazat-alágazat struktúrához. (2.ábra)

A modellnek továbbá tartalmaznia kell az egyes KI szervezeteknek a kritikusságát meghatározó kritériumokat, vagyis egy KI elvesztésének a

- hatókörét;
- nagyságrendjét és
- időbeni hatását.

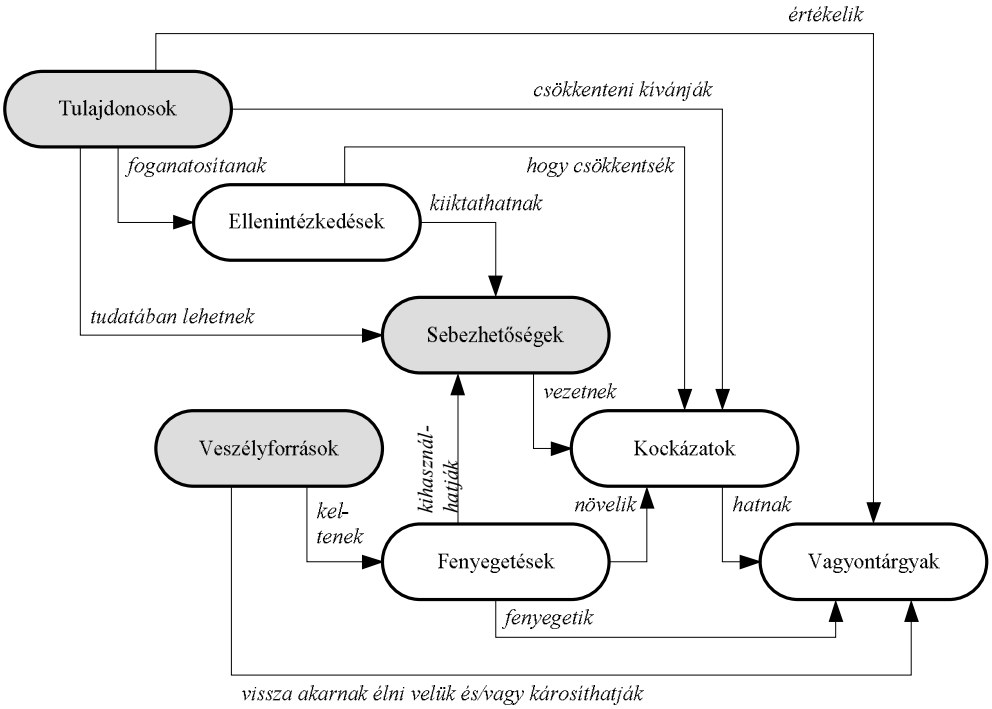
A hatókörnél meg kell vizsgálni, hogy a kritikus infrastruktúra, vagy annak részének elvesztése, elérhetetlensége milyen földrajzi kiterjedésben okoz károkat az állampolgárok gazdasági-, szociális jóléte, a közegészség, a közbiztonság, a nemzetbiztonság, a nemzetgazdaság és a kormányzat működése szempontjából. A nagyságrendnél meg kell vizsgálni, hogy a kritikus infrastruktúra vagy annak részének elvesztése, elérhetetlensége milyen mértékű hatást okoz. Az időbeni hatásnál pedig meg kell vizsgálni, hogy a kritikus infrastruktúra vagy annak részének elvesztése, elérhetetlensége milyen időtávon mennyi ideig befolyásolja az infrastruktúra újbóli működését. [1]



2. ábra. KI hierarchia modell struktúra UML objektum diagrammja
[Szerkesztették a szerzők]

A KI inter- és intradependenciáinak értékelése nem egy-egy gazdasági szervezet szintjén jelentkezik, és nem csak valamely állami szerv feladata, hanem össznemzeti védelmi feladat, ahol az államigazgatás, a nemzetvédelmi és az érintett gazdasági szervezetek hatékony és eredményes együttműködésével lehet teljeskörű, zárt és kockázatarányos védelmet kialakítani. Ennek a feltételnek a teljesítése miatt a modellnek lehetővé kell tennie a top-down elemzést (pl. a KI azonosítást és priorizálását) és a bottom-up tervezést (pl. az egyes KI elemek függőségeinek vizsgálatát, kapcsolatainak azonosítását).

A kockázatelemzésben felhasználandó elemzendő-objektumokra és azok általános kapcsolataira „Az informatikai biztonságértékelés közös szempontjai” (Common Criteria) ad egy a gyakorlatban is tesztelt és használható modellt:



3. ábra. Kockázatelemzés fogalmi modellje
[5: p 12.]

A fenti koncepció modellből látható, hogy a szűken vett kockázatelemzéshez a

- vagyontárgy;
- fenyegető tényező;
- kockázat;
- sebezhetőség és
- ellenintézkedés

elem-ötös meghatározása és értékelése szükséges.

A fenti ábrából az is jól látható, hogy a kockázatelemzést egy-egy vagyontárgy-fenyegetés párosra kell elvégezni, általánosságban (konkrét védendő érték hiányában) nincs értelme elemzésről beszélni. A modell alapján kimondható az is, hogy egy eredményes kockázatelemzéshez részletes erőforrás leltárra van szükség, illetve célszerű mind a veszélyforrások, mind az alkalmazott védelmi intézkedések listáját is törzsadatbázis elemként felvenni.

Jelen dolgozatunkban azonban – mivel a célunk nem a KI kockázatelemzés modellezése – a továbbiakban csak a KI függőséget közvetlenül befolyásoló kérdésekkel foglalkozunk.

Modellezési szintek

Az elemzés szempontjából megállapítható, hogy a függőségeket legpontosabban az egyes erőforrás-erőforrás kapcsolatok esetében lehet a legpontosabban modellezni, tényadatokat is ilyen szinten lehet begyűjteni, illetve szakértői becsléseket is az egyes rendszerelem kapcsolatok szintjén lehet végezni.

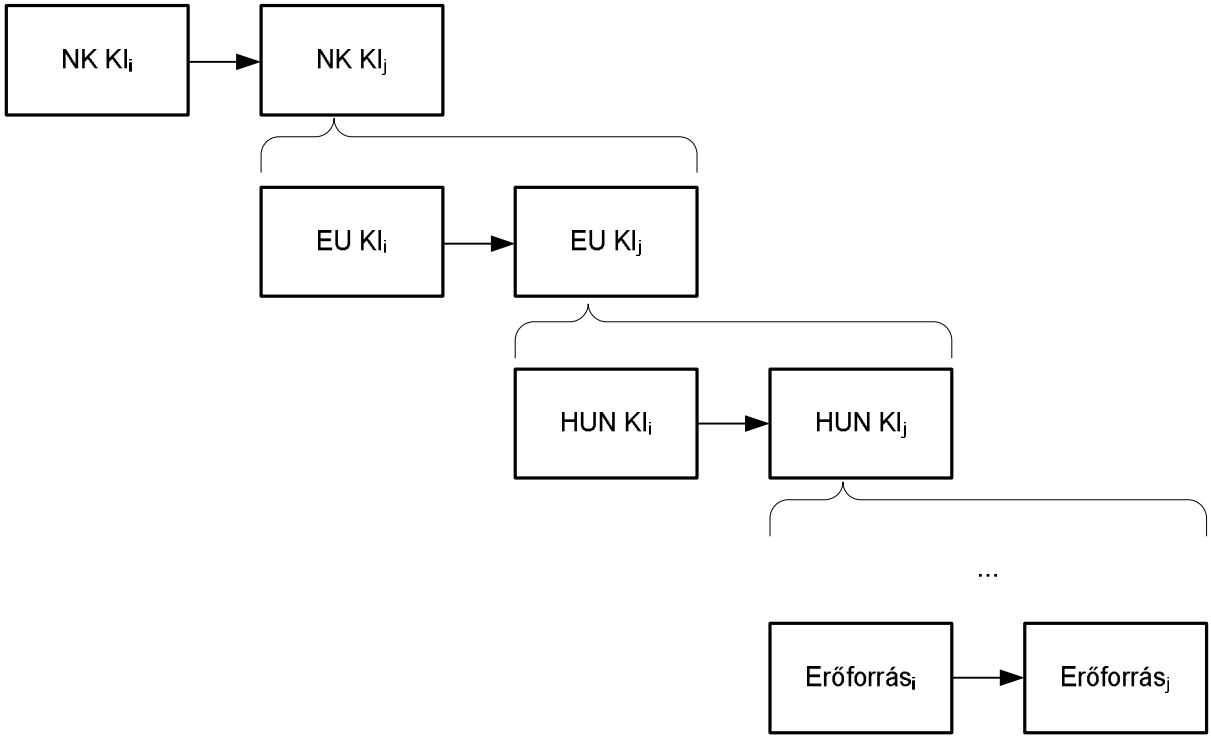
Modellezési szempontból fontos kérdés az is, hogy miként kezelhető egységes szemléletben a makro és mikro hierarchia, vagyis miként lehet azonos modell elemekkel leírni

a nemzetközi KI-KI dependenciákat, valamint egy szervezet erőforrásainak szintjén fellépő erőforrás-erőforrás dependenciákat.

A megoldáshoz az ötletet a virtuális vállalat (virtual business) koncepciója adta. [2] Ez egy olyan modellezési felfogás, amelyben egy szervezet a vele szoros kapcsolatban lévő más szervezetekkel együtt egy olyan egységet alkot, amelynek a belső kapcsolatrendszere (inter- és intradependenciái) egy külső szemlélő számára nem láthatók, az így kialakult organizáció egységes fellépése és működése helyettesíthető (és modellezhető) egy szervezettel, a tagszervezetek együtteséből felépített virtuális vállalattal.

Ilyen virtuális szervezetet alkot például az autógyár a beszállítóival együtt, ahol az együttműködés szoros keretei a JIT (just in time) módszertanra épülnek, vagy egy bank az összes kiszervezett funkciót ellátó szervezettel együtt.

Ilyen megközelítésben az egyes erőforrás kapcsolatokból felépíthető egy rendszer modellje, a rendszerek kapcsolataiból felépíthető egy szervezet, a szervezetekből felépíthető egy KI alágazat, az alágazatokból egy KI ágazat, illetve az alágazatokból, ágazatokból egy nemzeti, EU és nemzetközi KI is. Ezt a megközelítést szemlélteti a 4. ábra is.



Ahol:
NK KI – Nemzetközi kritikus infrastruktúra
EU KI – Európai Uniós kritikus infrastruktúra
HUN KI- Magyarországi/Nemzeti kritikus infrastruktúra
i..j – különböző infrastruktúrák, szervezetek, erőforrások, stb.

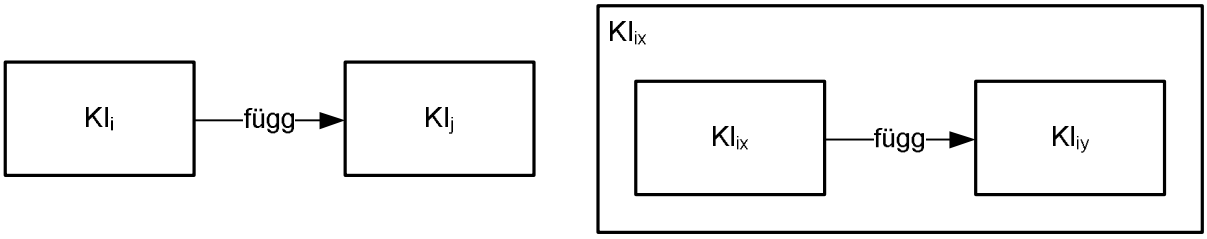
4. ábra. KI hierarchia, mint virtuális szervezetek kapcsolata
[Szerkesztették a szerzők]

Intradependencia – interdependencia

A szakirodalomban felmerül az inter- és intradependencia kérdése [3], amelyet modellezési szempontból is kezelni kell. Az interdependencia (a kölcsönös egymásra hatás) vizsgálata rendkívül fontos. Ennek során a vizsgált infrastruktúra más infrastruktúrákra gyakorolt

negatív hatását kell vizsgálni. Hangsúlyozni kell, hogy az interdependencia értékelése nagy fontossággal bír, mert ezek akár egy, akár több ágazat vagy alágazat bevonását illetve ezt követően együttes vizsgálatát követeli. A vizsgálat mennyiségi (kvantitatív) jellemzőkön alapul. [1]
Az interdependencia két KI közötti függést jelent (javasolt jelölése: $A \rightarrow B$, azaz „B" kritikus infrastruktúra elem függ „A" kritikus infrastruktúra elemtől). Az intradependencia egy adott KI önmagától való függését jelenti (javasolt jelölése: $A \rightarrow A$, azaz „A" kritikus infrastruktúra elem függ önmagától). Ez a függés rendszerint az „A" KI rendszernek saját belső al-KI rendszereinek függését jelenti.

Véleményünk szerint modellezési szempontból a KI rendszerek, alrendszerek közötti függés KI rendszerkomponensek közti függéseként értelmezhető és ábrázolható. Tehát a modell elemzési részlet finomításával az inter- és intradependencia ekvivalensként kezelhető, az intradependencia elhagyható, amit az 5. ábra b.) része szemléltet.
Ezt szemlélteti a következő ábra:



a.) Interdependencia b.) Intradependencia

Ahol:
KI_i, KI_j – különböző kritikus infrastruktúrák

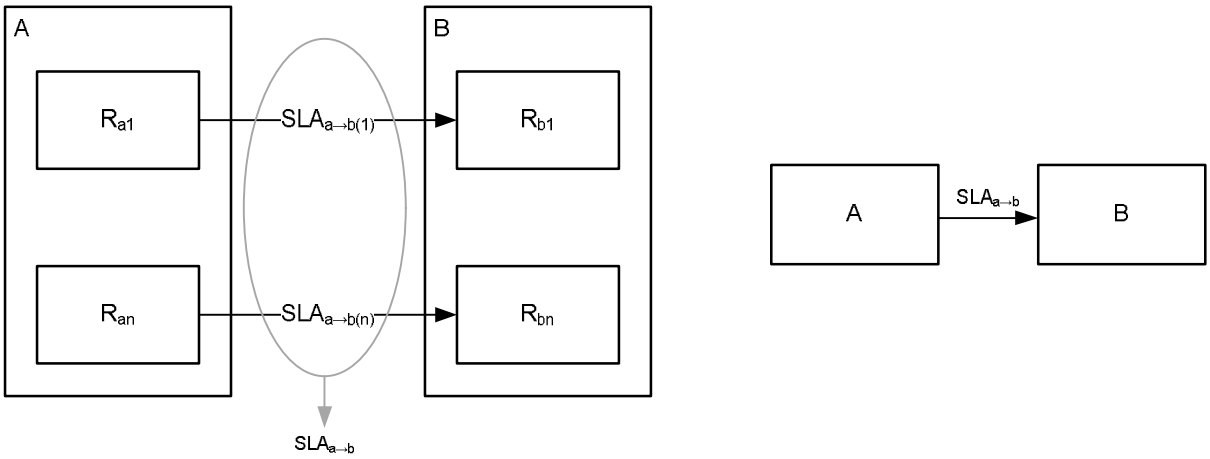
5. ábra. Inter és intradependencia helyettesítési modellje
[Szerkesztették a szerzők]

Függések modellezése

A KI-KI interdependencia vizsgálatának központi kérdése a függés. Ez a kapcsolat két rendszerelem között áll fenn, és mindkét irányból vizsgálható, egyrészt a függésben lévő rendszerelem, másrészt a függés alapjául szolgáló szolgáltatást nyújtó rendszerelem szempontjából.

Véleményünk szerint ez a függés modellezhető egy sajátos nyújtott-fogadott szolgáltatási szintmegállapodásként (SLA), amely azonban a rendelkezésre állással kapcsolatos metrikákat, valamint a szolgáltatás elmaradásának következményeit (hatás) tartalmazza. A szolgáltatás-alapú megközelítéssel kezelhető lenne az a probléma (is), hogy az alacsony modellezési szinten feltárt függőségeket egy magasabb elemzési szinten (szervezet-szervezet, alágazat-alágazat stb.) is értelmezni lehessen.

Javaslatunk alapján például egy szervezet-szervezet függőség felírható az igénybevevő szervezet számára szolgáltatást nyújtó alrendszerei szolgáltatásainak halmazaként (a két szervezet „szolgáltatási interfészén" keresztül nyújtott/fogadott szolgáltatások összegeként).



Ahol:
A,B – szervezetek
R_a,R_b – a szervezeteken belül szolgáltatást nyújtó alrendszerek
SLA – a rendszerek és/vagy szervezetek közötti nyújtott-fogadott szolgáltatási szintmegállapodások

6. ábra. KI szolgáltatási interfész egyedi függéseinek egyszerűsítése kumulált függéssel
[Szerkesztették a szerzők]

A függést leíró SLA javasolt tartalma „A kritikus információs infrastruktúrák meghatározásának módszertana” [1] alapján a következő:

	Alacsony	Közepes	Magas
Hatókör	0|1	0|1	0|1
Nagyságrend: a népességre gyakorolt hatás	0|1	0|1	0|1
Nagyságrend: a gazdasági hatás	0|1	0|1	0|1
Nagyságrend: interdependencia	0|1	0|1	0|1
Nagyságrend: politikai hatás	0|1	0|1	0|1
Időbeli hatás	0|1	0|1	0|1

7. ábra. KI SLA mátrix
[Szerkesztették a szerzők]

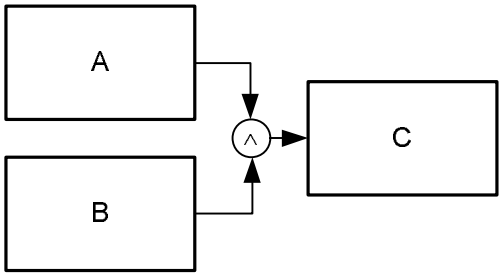
Hatás gráf felépítése

A valós életben a KI modellelemek kapcsolata rendszerint nem 1:1 típusú. Egy rendszerkomponens (pl. villamos hálózat) több más rendszerkomponens működéséhez nyújt alapvető szolgáltatást, illetve egy alkalmazás több egyéb rendszerkomponens működésétől függ (pl. az alkalmazást futtató hardvertől, operációsrendszertől, az adatokat szolgáltató adatbázis-kezelőtől, az ezek közti adatkapcsolathoz nélkülözhetetlen számítógépes hálózatoktól stb.).

A kapcsolatok n:m jellegének (azaz, hogy egy rendszerkomponenstől több más komponens is függhet, illetve, hogy egy rendszerkomponens több más komponenstől is függ) modellezéséhez hatás gráfok kialakítását javasoljuk (a támadási fákhoz hasonló szerkezetben), amelyek logikai kapcsolókkal fűzik össze az egyes rendszerelemek egymásra gyakorolt hatását. Az alapként szolgáló támadási fákkal szemben az így kialakított irányított háló (ahol az irányítást a nyújtott/fogadott szolgáltatás iránya adja meg) nem csak levél-

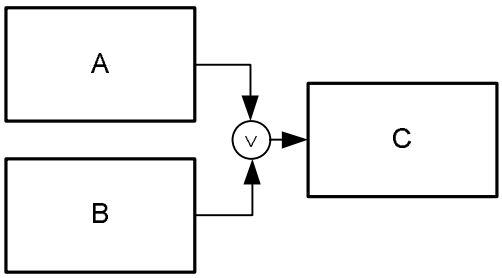
gyökér irányban járható be, hanem lehetséges valamennyi csomópont vizsgálata az abba vezető élek bejárásával.

A szolgáltatást igénybevevő rendszerkomponens funkcionalitásának, rendelkezésre állásának fenntartásához egymástól függetlenül is szükséges szolgáltatások esetére bevezettük az „és” kapcsolót, amelynek jelentése: „C” erőforrás működéséhez „A” és „B” erőforrások együttes szolgáltatása szükséges, bármelyikük kiesése „C” funkcionalitásának és rendelkezésre állásának sérülésével vagy megszűnésével jár együtt. Ezt a kapcsolatot szemlélteti a következő ábra:



8. ábra. „és” kapcsoló
[Szerkesztették a szerzők]

A szolgáltatást igénybevevő rendszerkomponens funkcionalitásának, rendelkezésre állásának fenntartásához egymást kiegészítő (redundáns) szolgáltatások esetére bevezettük a „vagy” kapcsolót, amelynek jelentése: „C” erőforrás működéséhez „A” vagy „B” erőforrások szolgáltatásai szükségesek, bármelyikük egyedüli kiesése nem jár együtt „C” funkcionalitásának és rendelkezésre állásának sérülésével. Ezt a kapcsolatot szemlélteti a következő ábra:



9. ábra. „vagy” kapcsoló
[Szerkesztették a szerzők]

Javaslatunk szerint a KI-KI rendszerelem kapcsolatok a formális logika, illetve a Fuzzy logika alapján kezelhetők, az irányított háló bejárásával. A háló bejárásával felderíthető, hogy egy adott rendszerelem mely más elemektől függ – tulajdonképpen az elemzés háló csomópontjai közti haladást jelenti a vizsgált elemtől visszafelé. A háló bejárásával azonosítható a függés tartalma és hatása, illetve áttételes függés esetén a függés „mélysége”, vagyis az, hogy hány élnyi távolságban van kritikus szolgáltatási elem az igénybevevőtől.

ÖSSZEFOGLALÁS

A kritikus infrastruktúrák, azok felmérése, kockázatelemzése napjaink egyik égető problémája. Az egyes KI ágazatok, alágazatok, szervezetek és egyedi eszközök, rendszerek kockázatelemzésének többféle módszertana létezik. Ezek lehetnek kvantitatív, kvalitatív módszerek, tartalmazhatnak több-kevesebb matematikai logikát, valószínűség számítást, lehetnek grafikusak, leíró jellegűek, egyszerűek, vagy bonyolultak. A KI-KI közötti függéseket, illetve egy KI-n belüli függéseket azonban ezek a modellek nem, vagy csak nagyon áttételesen kezelik.

Ennek a problémának a megoldására tettünk javaslatot a cikkünkben: egy olyan rendszerszemléletű modellt alkottunk meg, amely reményeink szerint alkalmas az inter- és intradependenciák modellezésére, a függőségek tartalmának feltérképezésére mind makro szinten (pl. KI ágazati vagy alágazati szinten), mind mikro szinten (az egyes rendszerelemek, alrendszerek szintjén). Az általunk javasolt megoldás a hagyományos kockázatelemzési modellek kiegészítésére is alkalmas lehet, hiszen az egyes erőforrások kockázati részmodelljét (ld. 2. és 3. ábra) egészíti ki egy félformális, a függőségeket és azok tartalmát is leíró modell.

Az általunk javasolt függőség elemzési módszert szeretnénk a jövőben egy informatikai alkalmazássá fejleszteni és egy részterület modellezésével validálni, ellenőrizni, hogy valós – komplex kapcsolatokkal rendelkező – rendszerek leírására is alkalmas-e.

Irodalomjegyzék

[1.] Dr. Haig Zsolt, Hajnal Béla, Dr. Kovács László, Dr. Muha Lajos, Sik Zoltán Nándor: A kritikus információs infrastruktúrák meghatározásának módszertana, http://www.cert-hungary.hu/downloads/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf, (2009.12.13.)

[2.] Virtual business. http://en.wikipedia.org/wiki/Virtual_business (2009.12.13.)

[3.] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, http://www.gdf.hu/html/Doktorans_Klub/documentums/DK01-Muha.pdf, (2009.12.13.)

[4.] Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research, http://www.inl.gov/technicalpublications/Documents/3489532.pdf, (2009.12.13.)

[5.] ISO/IEC 15408-1-3:2005: Information technology – Security techniques – Evaluation criteria for IT security

[6.] Szádeczky Tamás: Terrorizmus a kibertérben, Infokommunikáció és jog, 2008. V. évf. 6. sz. pp. 200-205.